|  |  |
| --- | --- |
| **مؤتمر المندوبين المفوضين (PP-22)بوخارست، 26 سبتمبر - 14 أكتوبر 2022** |  |
|  |  |
|  |  |
| الجلسة العامة | **الإضافة 7للوثيقة 44-A** |
|  | **3 يونيو 2022** |
|  | **الأصل: بالإنكليزية** |
|  |  |
| الدول الأعضاء في المؤتمر الأوروبي لإدارات البريد والاتصالات (CEPT) |
| المقترح الأوروبي المشترك 7 - مراجَعة القرار 130: |
| تعزيز دور الاتحاد في مجال بناء الثقة والأمنفي استخدام تكنولوجيا المعلومات والاتصالات |
|  |

MOD EUR/44A7/1

القـرار 130 (المراجَع في بوخارست، 2022)

تعزيز دور الاتحاد في مجال بناء الثقة والأمن
في استخدام تكنولوجيا المعلومات والاتصالات

إن مؤتمر المندوبين المفوضين للاتحاد الدولي للاتصالات (بوخارست، 2022)،

إذ يذكِّر

 *أ )* بالقرار 68/198 للجمعية العامة للأمم المتحدة، بشأن تسخير تكنولوجيات المعلومات والاتصالات (ICT) لأغراض التنمية؛

*ب)* بالقرار 71/199 للجمعية العامة للأمم المتحدة، بشأن الحق في الخصوصية في العصر الرقمي؛

*ج)* بالقرار 68/243 للجمعية العامة للأمم المتحدة، بشأن التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي؛

*د )* بالقرار 57/239 للجمعية العامة للأمم المتحدة، بشأن إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي؛

*ﻫ )* بالقرار 64/211 للجمعية العامة للأمم المتحدة، بشأن إرساء ثقافة عالمية تكفل أمن الفضاء الإلكتروني وتقييم الجهود الوطنية الرامية إلى حماية الهياكل الأساسية الحيوية للمعلومات؛

*و )* بالقرار 70/125 للجمعية العامة للأمم المتحدة، بشأن الوثيقة الختامية للاجتماع الرفيع المستوى للجمعية العامة بشأن الاستعراض العام لتنفيذ نتائج القمة العالمية لمجتمع المعلومات؛

*ز )* بالقرار 70 (المراجَع في بوخارست، 2022) لمؤتمر المندوبين المفوضين، بشأن تعميم مبدأ المساواة بين الجنسين في الاتحاد وترويج المساواة بين الجنسين وتمكين المرأة من خلال الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*ح)* بالقرار 174 (المراجَع في بوسان، 2014) لمؤتمر المندوبين المفوضين، بشأن دور الاتحاد الدولي للاتصالات في قضايا السياسة العامة الدولية المتعلقة بمخاطر الاستعمال غير القانوني لتكنولوجيا المعلومات والاتصالات؛

*ط)* بالقرار 179 (المراجَع في دبي، 2018) لهذا المؤتمر، بشأن دور الاتحاد في حماية الأطفال على الخط؛

*ي)* بالقرار 181 (المراجَع في غوادالاخارا، 2010) لمؤتمر المندوبين المفوضين، بشأن التعاريف والمصطلحات المتعلقة ببناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

*ك)* بالقرار 196 (المراجَع في دبي، 2018) لهذا المؤتمر، بشأن حماية مستعملي/مستهلكي خدمات الاتصالات؛

*ل)* بالقرار 140 (المراجَع في دبي، 2018) لهذا المؤتمر، بشأن دور الاتحاد في تنفيذ نتائج القمة العالمية لمجتمع المعلومات وفي الاستعراض الشامل للجمعية العامة للأمم المتحدة لتنفيذها؛

*م )* بالنتائج ذات الصلة لقطاعات الاتحاد الثلاثة والقرارات الصادرة عن مؤتمراتها،

وإذ يضع في اعتباره

 *أ )* أن الاتصالات/تكنولوجيا المعلومات والاتصالات قد أدت دوراً هاماً وإيجابياً في التعامل مع آثار جائحة كوفيد-19 ولكن المخاطر السيبرانية قد ازدادت مع انتقال المزيد من الأنشطة إلى الإنترنت؛

*ب)* أن زيادة العمل عبر الإنترنت خلال الجائحة زادت من أهمية قيام المنظمات بوضع حلول فعالة للشبكات وضوابط للنفاذ وإدارة آمنة عن بعد للأجهزة وتقديم إرشادات للمستعملين؛

*ج)* أن الاتحاد أدى دوراً قيماً خلال الجائحة حيث وفر منصة للمنظمين وواضعي السياسات وأصحاب المصلحة الآخرين المعنيين بتكنولوجيا المعلومات والاتصالات لتبادل المعلومات وأفضل الممارسات، من خلال المنصة العالمية للاتحاد بشأن قدرة الشبكات على الصمود، على سبيل المثال؛

*د )* أن الحدث الرفيع المستوى WSIS+10 الذي نسقه الاتحاد أكد من جديد أهمية بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، على النحو المشار إليه في الفقرات ذات الصلة من الوثائق الختامية للحدث WSIS+10 (جنيف، 2014)؛

*هـ )* الأهمية البالغة للبنية التحتية للمعلومات والاتصالات وتطبيقاتها بالنسبة إلى جميع أشكال النشاط الاجتماعي والاقتصادي تقريباً؛

*و )* الأحكام المتصلة بالأمن السيبراني في التزام تونس وبرنامج عمل تونس والوثيقة الختامية للاجتماع رفيع المستوى للجمعية العامة للأمم المتحدة بشأن الاستعراض العام لتنفيذ نتائج القمة العالمية لمجتمع المعلومات؛

*ز )* أن تهديدات جديدة من مختلف المصادر تظهر مع تطبيق وتنمية تكنولوجيا المعلومات والاتصالات وأن هذه التهديدات تؤثر على الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات من جانب جميع الدول الأعضاء وأعضاء القطاعات وأصحاب المصلحة الآخرين، بمن فيهم جميع مستعملي تكنولوجيا المعلومات والاتصالات، إلى جانب أثرها في الحفاظ على السلام وفي التنمية الاقتصادية والاجتماعية لجميع الدول الأعضاء، وأن التهديدات ومواطن الضعف التي تعاني منها البنية التحتية والشبكات والأجهزة لا تزال تثير تحديات أمنية متزايدة عبر الحدود الوطنية تواجهها جميع البلدان، وخاصة البلدان النامية، ويلاحظ في الوقت نفسه في هذا السياق تعزيز دور الاتحاد الدولي للاتصالات في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات وضرورة مواصلة تعزيز التعاون الدولي وبناء القدرات وتطوير وتكييف الآليات الوطنية والإقليمية والدولية الملائمة الموجودة حالياً (مثل الاتفاقات، وأفضل الممارسات، ومذكرات التفاهم، وما إلى ذلك)؛

*ح)* أنه تمت دعوة الأمين العام للاتحاد لدعم مشاريع عالمية وإقليمية أخرى للأمن السيبراني، حسب الاقتضاء، كما أن جميع البلدان، خاصة البلدان النامية، وجهت إليها الدعوة للمشاركة في أنشطتها ذات الصلة بالاتحاد الدولي للاتصالات؛

*ط)* البرنامج العالمي للأمن السيبراني (GCA) للاتحاد الدولي للاتصالات، الذي يشجع التعاون الدولي الهادف إلى اقتراح استراتيجيات لإيجاد حلول من أجل تعزيز الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*ي)* أن حماية هذه البنية التحتية والتصدي لهذه التحديات والتهديدات يتطلبان إجراءات وطنية وإقليمية ودولية منسقة من أجل منع وقوع أي حادث مرتبط بأمن الحواسيب والاستعداد له والاستجابة له والتغلب عليه من جانب السلطات الحكومية على الأصعدة الوطنية (بما في ذلك إنشاء أفرقة وطنية للاستجابة للحوادث الحاسوبية)، ودون الوطنية، ومن جانب القطاع الخاص والمواطنين والمستعملين، كما يتطلبان التعاون والتنسيق على الصعيدين الدولي والإقليمي، وأن على الاتحاد الاضطلاع بدور ريادي في هذا المجال، في إطار اختصاصاته وكفاءاته؛

*ك)* أن النهج التكراري والقائم على المخاطر للأمن السيبراني يمكّن من تطوير وتطبيق ممارسات الأمن السيبراني بطريقة حسب الحاجة من أجل التصدي للتهديدات ومواطن الضعف المتغيرة باستمرار، وأن الأمن هو عملية متواصلة ومتكررة يجب أن تكون في صلب تطور (عن طريق مراعاة الأمن في التصميم مثلاً) ونشر التكنولوجيات وتطبيقاتها من البداية وأن تستمر طوال دورة حياتها؛

*ل)* الحاجة إلى إحراز تقدم مستمر في التكنولوجيات الحديثة لدعم منع الأحداث أو الحوادث التي تؤثر على أمن الحواسيب أو الحوادث المتعلقة بأمن الشبكات الحاسوبية والتي من شأنها تقويض توفر البنى التحتية الحرجة وسلامتها وسريتها والكشف المبكر عنها والاستجابة لها في الوقت المناسب، في الدول الأعضاء في الاتحاد والحاجة إلى استراتيجيات تتيح الحد من احتمال وأثر هذه الحوادث وتخفيف المخاطر والتهديدات المتنامية التي تتعرض لها هذه المنصات؛

*م )* أن القرار 70/125 للجمعية العامة للأمم المتحدة، الوثيقة الختامية للاجتماع الرفيع المستوى للجمعية العامة بشأن الاستعراض العام لتنفيذ نتائج القمة العالمية لمجتمع المعلومات (WSIS)، يقر بالتحديات التي تواجهها البلدان، خاصةً البلدان النامية، في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات وينادي بالتركيز مجدداً على بناء القدرات والتعليم وتبادل المعارف والممارسات التنظيمية إضافةً إلى تعزيز التعاون بين أصحاب المصلحة المتعددين على جميع المستويات وزيادة الوعي بين مستعملي تكنولوجيا المعلومات والاتصالات، خاصةً بين الفئات الأكثر فقراً والأشد ضعفاً؛

*ن)* أن عدد وحجم التهديدات السيبرانية والهجمات السيبرانية يتزايد، ويزداد أيضاً الاعتماد على تكنولوجيات المعلومات والاتصالات الضرورية لأغراض النفاذ إلى الخدمات والمعلومات؛

*س)* أن واقع معايير الأمن السيبراني بطبيعته يتطلب التعاون بين الاتحاد الدولي للاتصالات والمنظمات الوطنية والإقليمية والعالمية والقطاعية الأخرى؛

*ع)* أن هذا المشهد يمكن أن يكون معقداً ويمكن للاتحاد أن يؤدي دوراً هاماً في إذكاء الوعي بين الأعضاء بالعمل ذي الصلة في المنظمات الأخرى وبالعمليات والمبادرات الرامية إلى تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

*ف)* أن الاتحاد يمكنه أن يؤدي دوراً هاماً في إذكاء الوعي بين المنظمات الأخرى المعنية والعمليات والمبادرات بالتحديات الخاصة التي تواجهها البلدان النامية في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

*ص)* أن العديد من البلدان النامية تضع أو تنفذ استراتيجيات وطنية للأمن السيبراني؛

*ق)* أن هناك حاجة إلى أن تنطوي مهنة الأمن السيبراني على مؤهلات قوية وفعالة ومسارات مهنية أكثر وضوحاً لتشجيع المزيد من الأشخاص على الانضمام إلى المهنة، وضمان إمكانية النفاذ إلى البرامج التدريبية وفعاليتها ودعم أصحاب العمل لتوظيف الأشخاص ذوي المهارات والخبرة المناسبة؛

*ر )* أنه على الرغم من التقدم المحرز في بعض المجالات، يواجه العديد من البلدان تحديات في تطوير مؤهلات ومسارات مهنية فعالة، وهذا يشكل عائقاً كبيراً أمام تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

*ش)* أن الأمن السيبراني أصبح مسألة في غاية الأهمية على الصعيد الدولي وبالتالي، فإن دور ومشاركة الأمم المتحدة ووكالاتها المتخصصة ذات الصلة، من قبيل الاتحاد الدولي للاتصالات، في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، يتسمان بالأهمية؛

*ت)* الأدوار والمسؤوليات المختلفة لجميع أصحاب المصلحة في ضمان الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*ث)* أن بعض الشركات الصغيرة والمتوسطة تواجه تحديات إضافية في تنفيذ ممارسات الأمن السيبراني؛

*خ)* الحاجة إلى زيادة وعي الجمهور بمخاطر الأمن السيبراني التي قد يواجهها، بما في ذلك في المجتمعات النائية والريفية والتي تفتقر إلى الخدمات والفئات الضعيفة؛

*ذ )* الحاجة إلى تعزيز الخطوات الأساسية التي ينبغي لجميع أفراد الجمهور اتخاذها لحماية أنفسهم من مخاطر الأمن السيبراني، مثل استعمال كلمات سر قوية والاستيقان بعامليْن وتحديث البرمجيات بصورة منتظمة؛

وإقراراً منه

 *أ )* بأن الأمن السيبراني عنصر أساسي لتأمين البنى التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات، كما أنه ركيزة أساسية بالنسبة إلى التنمية الاجتماعية والاقتصادية؛

*ب)* بأن تطوير تكنولوجيا المعلومات والاتصالات كان ولا يزال عاملاً حاسماً في نمو الاقتصاد العالمي، بما في ذلك الاقتصاد الرقمي وتنميته على أساس من الأمن والثقة؛

*ج)* بأن الاتصالات/تكنولوجيا المعلومات والاتصالات تمكّن من تنمية المجتمع المدني وتسهم في تحقيق مستويات أعلى من المنافع الاجتماعية والإدماج الاجتماعي، وتوفر قنوات جديدة بين المواطنين والشركات والحكومات لتبادل المعارف وتعزيزها، فضلاً عن المشاركة في اتخاذ القرارات التي تؤثر على حياتهم وعملهم؛

*د )* بأن القمة العالمية لمجتمع المعلومات أكدت على أهمية بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات والأهمية الكبرى لأعمال التنفيذ من جانب أصحاب المصلحة المتعددين على الصعيد الدولي، وأنها وضعت خط العمل جيم5 (بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات) وحددت دور الاتحاد في برنامج عمل تونس بشأن مجتمع المعلومات ليقوم بمهمة تنسيق/تيسير تنفيذ هذا الخط وأقرت باضطلاع الاتحاد بهذه المهمة في السنوات الأخيرة، من خلال البرنامج العالمي للأمن السيبراني على سبيل المثال؛

*هـ )* بالفقرة 15 من التزام تونس التي تنص على ما يلي: *"مع الاعتراف بمبادئ النفاذ الشامل وغير التمييزي إلى تكنولوجيا المعلومات والاتصالات لجميع البلدان وبضرورة مراعاة مستوى التنمية الاجتماعية والاقتصادية لكل بلد واحترام نواحي مجتمع المعلومات ذات التوجه التنموي، فإننا نؤكد على أن تكنولوجيا المعلومات والاتصالات هي أداة فعالة في تعزيز السلام والأمن والاستقرار والديمقراطية والتلاحم الاجتماعي والإدارة الرشيدة وحكم القانون، على المستويات الوطنية والإقليمية والدولية. ويمكن الاستفادة من تكنولوجيا المعلومات والاتصالات في تعزيز النمو الاقتصادي ونمو المؤسسات. وندرك أن النهوض بالبنية التحتية وبناء القدرات البشرية وأمن المعلومات وأمن الشبكات كلها أمور حيوية في تحقيق هذه الغايات. ونعترف كذلك بضرورة المواجهة الفعالة للتحديات والتهديدات الناتجة عن استخدام تكنولوجيا المعلومات والاتصالات لأغراض لا تتفق مع أهداف حفظ الاستقرار والأمن الدوليين وبأنها يمكن أن تؤثر تأثيراً سيئاً على تكامل البنية التحتية في داخل الدول، مما يؤثر على أمن تلك الدول. لذلك من الضروري أن نعمل على منع إساءة استخدام موارد المعلومات وتكنولوجيا المعلومات لأغراض إجرامية وإرهابية، وذلك مع احترام حقوق الإنسان"*، وأن التحديات الناجمة عن سوء استعمال موارد تكنولوجيا المعلومات والاتصالات استمرت في الازدياد منذ انعقاد القمة العالمية لمجتمع المعلومات؛

*و )* بأن الدول الأعضاء، ولا سيما البلدان النامية، قد تحتاج، لدى وضع تدابير قانونية مناسبة وعملية بشأن الحماية من التهديدات السيبرانية على المستويات الوطنية والإقليمية والدولية، إلى مساعدة من الاتحاد في وضع تدابير تقنية وإجرائية، الهدف منها ضمان أمن البنى التحتية الوطنية لتكنولوجيا المعلومات والاتصالات، وذلك بناءً على طلب هذه الدول الأعضاء، مع ملاحظة أن هناك عدداً من المبادرات الوطنية والدولية التي قد تدعم هذه البلدان لإعداد مثل هذه التدابير القانونية؛

*ز )* بأن الشبكات الآمنة والموثوقة من شأنها بناء الثقة والتشجيع على تبادل واستخدام المعلومات والبيانات؛

*ح)* بأن تنمية المهارات البشرية وبناء القدرات يشكلان عنصرين رئيسيين في تعزيز حماية شبكات المعلومات؛

*ط)* بأن العديد من الدول الأعضاء تواجه نقصاً كبيراً في المهارات في القوى العاملة لديها في مجال الأمن السيبراني، وأن هذا النقص في المهنيين المتمرسين في مجال الأمن السيبراني يشكل عائقاً أساسياً أمام بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

*ي)* بأن العديد من الدول الأعضاء تواجه اختلالاً كبيراً في التوازن بين الجنسين في القوى العاملة لديها في مجال الأمن السيبراني، وهذا يزيد من صعوبة معالجة نقص المهارات؛

*ك)* بأن القرار 70 لمؤتمر المندوبين المفوضين يقرّ بأن الضرورة تقتضي من أعضاء الاتحاد وشركائه تشجيع الفتيات على اختيار مسار وظيفي في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات، ويشجع الدول الأعضاء وأعضاء القطاعات على تيسير توظيف الرجال والنساء على قدم المساواة في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات، ويدعو الدول الأعضاء وأعضاء القطاعات إلى تقديم الدعم اللازم بحيث يتسنى للنساء والفتيات القيام بدراسات والعمل في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات؛

*ل)* بأن من المهم تشجيع المزيد من الناس، ولا سيما النساء والفتيات، على اختيار مسار وظيفي في مجال الأمن السيبراني من أجل معالجة نقص المهارات؛

*م )* بأن الدول الأعضاء تبذل جهوداً لتحسين البيئات المؤسسية؛

*ن)* بأن عمليات تقييم المخاطر وتحليلها توفر فهماً أفضل لمخاطر الأمن السيبراني التي تواجهها المنظمات وكيفية تخفيف أثرها؛

*س)* بأهمية أن تشجع الدول الأعضاء الإبلاغ بشكل مسؤول عن مواطن الضعف في تكنولوجيا المعلومات والاتصالات وتبادل المعلومات بشأن كيفية معالجة مواطن الضعف هذه،

وإذ يدرك

 *أ )* أن الاتحاد الدولي للاتصالات والمنظمات الدولية الأخرى تقوم، من خلال مجموعة منوعة من الأنشطة، بفحص المسائل المتصلة ببناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، بما في ذلك الاستقرار وتدابير مكافحة الرسائل الاقتحامية والبرمجيات الضارة وما إلى ذلك، إلى جانب حماية البيانات الشخصية والخصوصية؛

*ب)* أن للاتحاد عدد من الأدوار الأساسية التي ينبغي أن يضطلع بها في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*ج)* أن الاتحاد يساعد أيضاً البلدان النامية في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات ويدعم إنشاء أفرقة الاستجابة للحوادث الحاسوبية، بما في ذلك أفرقة استجابة للحوادث الحاسوبية تكون مسؤولة عن التعاون بين الحكومات، وأهمية التنسيق بين جميع المنظمات ذات الصلة،

وإذ يلاحظ

 *أ )* أن الاتحاد، بصفته منظمة دولية حكومية يشارك فيها القطاع الخاص، يحتل مركزاً يسمح له بأن يقوم بدور هام، مشتركاً مع المنظمات والهيئات الدولية الأخرى، في التصدي للتهديدات ومواطن الضعف التي تؤثر على بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*ب)* الفقرتين 35 و36 من إعلان مبادئ جنيف والفقرة 39 من برنامج عمل تونس بشأن بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*ج)* أنه رغم عدم وجود تعاريف متفق عليها عالمياً للرسائل الاقتحامية وغير ذلك من العبارات في هذا المجال، فقد وصفت لجنة الدراسات 2 لقطاع تقييس الاتصالات، في اجتماعها في يونيو 2006، الرسائل الاقتحامية بأنها عبارة تُستعمل عموماً لتصف الرسائل الإلكترونية غير المرغوبة التي تصل بحجم كبير في البريد الإلكتروني أو نظام رسائل الهاتف المحمول، وغايتها تسويق منتجات أو خدمات تجارية؛

*د )* مبادرة الاتحاد المتعلقة بالتعاون مع منتدى أفرقة الأمن والاستجابة للحوادث (FIRST)،

يقرر

1 تهنئة الاتحاد على المنصة العالمية بشأن قدرة الشبكات على الصمود وعمله لتوفير منصة للمنظمين وواضعي السياسات وأصحاب المصلحة الآخرين المعنيين بتكنولوجيا المعلومات والاتصالات لتبادل المعلومات وأفضل الممارسات بشأن الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات للتخفيف من آثار جائحة فيروس كورونا (كوفيد-19)؛

2 أن يستمر في إيلاء هذا العمل أولوية عالية داخل الاتحاد طبقاً لاختصاصاته وخبراته، بما في ذلك تعزيز الفهم المشترك بين الحكومات وأصحاب المصلحة الآخرين بشأن بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات على الصعيد الوطني والإقليمي والدولي؛

3 أن يعطي أولوية عالية للعمل الجاري في الاتحاد والموصوف في فقرة *"إذ* *يأخذ في الاعتبار"* أعلاه، طبقاً لاختصاصاته ومجالات خبراته، وأن يواصل العمل عن كثب، حسب الاقتضاء، مع الهيئات/الوكالات الأخرى ذات الصلة التابعة للأمم المتحدة والهيئات الدولية الأخرى ذات الصلة، مع مراعاة الولايات المحددة ومجالات الخبرة لمختلف الوكالات مع التنبه إلى الحاجة إلى تفادي ازدواج الأعمال بين المنظمات وبين المكاتب أو الأمانة العامة؛

4 أن يركز الاتحاد موارده وبرامجه على مجالات الأمن السيبراني الوطنية والإقليمية والدولية التي تندرج ضمن اختصاصاته وخبراته الأساسية، وتحديداً الجوانب التقنية والتنموية، مع استبعاد المجالات المتعلقة بتطبيق الدول الأعضاء لمبادئ قانونية أو سياساتية تتعلق بالدفاع والأمن الوطنيين والمحتوى والجريمة السيبرانية والتي تشملها الحقوق السيادية لهذه الدول، بيد أن ذلك لا يستثني الاتحاد من الاضطلاع بولايته المتعلقة بوضع توصيات تقنية معدة للحد من أوجه الضعف في البنية التحتية لتكنولوجيا المعلومات والاتصالات، كما لا يستثني ذلك الاتحاد من توفير المساعدة المتفق عليها في المؤتمر العالمي لتنمية الاتصالات لعام 2017 بما في ذلك في إطار الهدف 2 والأنشطة ذات الصلة بالمسألة 3/2؛

5 تشجيع ثقافة يُنظر فيها إلى الأمن كعملية مستمرة ومتكررة تُدمج في المنتجات منذ بداية استخدامها وتستمر طوال فترة عمرها ويتسنى للمستعملين النفاذ إليها وفهمها؛

6 تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات بطريقة تتيح تنمية المجتمع المدني وتدعم تحقيق مستويات أعلى من المنافع الاجتماعية والاندماج الاجتماعي؛

7 تعزيز زيادة وعي أعضاء الاتحاد بالأنشطة المضطلع بها في الاتحاد والكيانات الأخرى ذات الصلة المشاركة في تعزيز الأمن السيبراني، بما في ذلك أنشطة بناء القدرات؛

8 التواصل بفعالية مع المنظمات الأخرى ذات الصلة لإذكاء وعيها بالتحديات الخاصة التي تواجهها البلدان النامية في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات؛

9 المساهمة في مواصلة تعزيز الثقة وإطار الأمن، بما يتسق مع دور الاتحاد بوصفه جهة التيسير الرئيسية لخط العمل جيم5 للقمة العالمية لمجتمع المعلومات، مع مراعاة القرار 140 (المراجَع في دبي، 2018) لهذا المؤتمر؛

10 الاستمرار، استناداً إلى قاعدة المعلومات المرتبطة "بخارطة الطريق الخاصة بمعايير أمن تكنولوجيا المعلومات والاتصالات"وجهود قطاع تنمية الاتصالات بشأن الأمن السيبراني، وبمساعدة المنظمات الأُخرى ذات الصلة، في تحديث قائمة المبادرات والأنشطة الوطنية والإقليمية والدولية لتشجيع وضع نهج مشتركة في مجال الأمن السيبراني؛

11 تعزيز نمو وتطوير قوى عاملة متنوعة ومتمرسة في مجال الأمن السيبراني، قادرة على معالجة وتخفيف المخاطر السيبرانية، بوسائل منها تطوير مؤهلات ومسارات مهنية فعّالة؛

12 إعداد دراسات حالة عن الترتيبات المؤسسية المتعلقة بالأمن السيبراني، والنهج التنظيمية، وبرامج التوعية، والمهارات وتنمية القوى العاملة، بالتعاون مع الأعضاء ومع المنظمات ذات الصلة؛

13 النظر في التحديات الخاصة بالأمن السيبراني التي تواجهها الشركات الصغيرة والمتوسطة وإدراج هذه الاعتبارات في أنشطة الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

14 مراعاة أثر نشر التكنولوجيات الناشئة على الأمن السيبراني، بما في ذلك التكنولوجيات الجديدة لأمن الشبكات وإدراج تلك الاعتبارات في أنشطة الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

15 دعم تطوير البنية التحتية التي يرتكز عليها التحول الرقمي الجاري للاقتصاد العالمي من خلال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، خاصةً في التصدي للتهديدات الحالية والمستقبلية، وذلك في إطار ولاية الاتحاد؛

16 استخدام إطار البرنامج العالمي للأمن السيبراني للاتحاد لمواصلة توجيه عمل الاتحاد بشأن الجهود الرامية إلى بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات،

يكلف الأمين العام ومديري المكاتب

1بمواصلة توفير منصة للمنظمين وواضعي السياسات وأصحاب المصلحة الآخرين المعنيين بتكنولوجيا المعلومات والاتصالات من أجل تبادل المعلومات وأفضل الممارسات بشأن الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات للتخفيف من آثار جائحة فيروس كورونا (كوفيد-19)؛

2 بمواصلة استعراض:

’1‘ العمل المنجز حتى الآن في القطاعات الثلاثة للاتحاد وفي إطار البرنامج العالمي للأمن السيبراني للاتحاد والمنظمات الأخرى المعنية ومبادرات التصدي للتهديدات القائمة والمقبلة وتعزيز الحماية منها، من أجل بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

’2‘ التقدم المحرز في تنفيذ هذا القرار، مع مواصلة الاتحاد دوره كجهة التنسيق/التيسير الرئيسية لخط العمل جيم5 للقمة العالمية، وذلك بمساعدة الأفرقة الاستشارية وبما يتماشى مع دستور الاتحاد واتفاقيته؛

’3‘ نتائج العمل المنجز حتى الآن في دعم البلدان النامية خصوصاً، في مجال بناء القدرات والمهارات المتعلقة بالأمن السيبراني للتأكد من أن الاتحاد يركز موارده بشكل فعّال للتصدي لتحديات التنمية؛

3 بتقديم تقرير إلى المجلس، بما يتفق والقرار 45 (المراجَع في دبي، 2014)، بشأن الأنشطة الجارية في الاتحاد والمنظمات والكيانات الأخرى ذات الصلة لتعزيز التعاون والعمل المشترك، على الصعيدين الإقليمي والعالمي، وتعزيز بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات للدول الأعضاء، ولا سيما البلدان النامية، مع مراعاة أي معلومات تقدمها الدول الأعضاء، بما في ذلك معلومات عن الحالات التي تقع ضمن ولايتها ويمكن أن تؤثر على هذا التعاون؛

4 بتقديم تقرير عن مذكرات التفاهم (MoU) بين البلدان المعنية، بما يتفق والقرار 45 (المراجَع في دبي، 2014) علاوةً على أشكال التعاون القائمة، مع تقديم تحليل عن حالتها ونطاقها وتطبيقات آليات التعاون هذه لتعزيز الأمن السيبراني ومكافحة التهديدات السيبرانية، بغية تمكين الدول الأعضاء من تحديد مدى الاحتياج إلى مزيدٍ من المذكرات أو الآليات؛

5 بإذكاء الوعي بشأن الأنشطة المضطلع بها داخل الاتحاد والكيانات الأخرى ذات الصلة المشاركة في تعزيز الأمن السيبراني، بما في ذلك أنشطة بناء القدرات، والتحديات الخاصة التي تواجهها البلدان النامية، في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات بما يتماشى مع الفقرتين 7 و8 من *"يقرر"*؛

6بتسهيل النفاذ إلى الأدوات والموارد المطلوبة، في حدود الميزانية المتاحة، لتعزيز الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات لصالح جميع الدول الأعضاء، وذلك تماشياً مع أحكام القمة العالمية بشأن النفاذ الشامل وغير التمييزي إلى تكنولوجيا المعلومات والاتصالات أمام جميع البلدان؛

7 بمواصلة تبادل المعارف والمعلومات عن المبادرات الوطنية والإقليمية والدولية المتصلة بالأمن السيبراني الحالية والمستقبلية في أنحاء العالم عن طريق الصفحة الإلكترونية للأمن السيبراني للاتحاد وتشجيع جميع أصحاب المصلحة على المساهمة في هذه الأنشطة، مع مراعاة البوابات الإلكترونية القائمة؛

8 بتقديم تقرير سنوي إلى المجلس عن هذه الأنشطة وعرض مقترحات حسب الاقتضاء؛

9 بمواصلة تعزيز التنسيق بين لجان الدراسات والبرامج المعنية،

يكلف مدير مكتب تقييس الاتصالات

1 بتكثيف الأعمال في لجان دراسات القطاع القائمة حالياً بغية:

’1‘ التصدي للتهديدات ومواطن الضعف القائمة والمقبلة التي تؤثر على جهود بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، مع مراعاة الخدمات الجديدة والتطبيقات الناشئة القائمة على شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات، من خلال إعداد تقارير أو توصيات حسب الاقتضاء، بهدف تنفيذ قرارات الجمعية العالمية لتقييس الاتصالات، لا سيما القرارات 50 و52 (المراجعَين في الحمامات، 2016) و58 (المراجَع في دبي، 2012) التي تتيح البدء بالعمل قبل الموافقة على المسألة؛

’2‘ التماس الطرق لتعزيز تبادل المعلومات التقنية في هذه المجالات، وتعزيز اعتماد البروتوكولات والمعايير التي تزيد من تعزيز الأمن وتشجع التعاون الدولي بين الهيئات ذات الصلة؛

’3‘ تسهيل المشاريع المنبثقة عن نتائج الجمعية العالمية لتقييس الاتصالات، لا سيما:

• القرار 50 (المراجَع في الحمامات، 2016)، بشأن الأمن السيبراني؛

• القرار 52 (المراجَع في دبي، 2012)، بشأن التصدي للرسائل الاقتحامية ومكافحتها؛

2 بالنظر داخل قطاع تقييس الاتصالات في تشجيع ثقافة ينظر فيها إلى الأمن كعملية مستمرة ومتكررة وتقديم مقترحات إلى المجلس حسب الاقتضاء؛

3 بمواصلة التعاون مع المنظمات المعنية بغية تبادل أفضل الممارسات ونشر المعلومات من خلال ورش عمل ودورات تدريبية مشتركة وأفرقة أنشطة تنسيق مشتركة ومن خلال مساهمات خطية من المنظمات ذات الصلة بناءً على دعوات توجه إليها، على سبيل المثال،

يكلف مدير مكتب تنمية الاتصالات

1 بأن يقوم، بما يتفق مع نتائج المؤتمر العالمي لتنمية الاتصالات لعام 2022 وعملاً بالقرارات 45 (المراجَع في كيغالي، 2022) و69 (المراجَع في كيغالي، 2022) و80 (المراجَع في بوينس آيرس، 2017) وأولوية قطاع تنمية الاتصالات الواردة في خطة عمل كيغالي والمتمثلة في *الاتصالات/تكنولوجيا المعلومات والاتصالات الآمنة والشاملة للجميع لتحقيق التنمية المستدامة*، بدعم المشاريع الإقليمية والعالمية بشأن الأمن السيبراني وتشجيع جميع البلدان على المشاركة في هذه الأنشطة؛

2 بدعم الدول الأعضاء في الاتحاد، بناءً على طلبها، في جهودها الرامية إلى بناء القدرات من خلال تسهيل نفاذ الدول الأعضاء إلى الموارد التي طورتها المنظمات الدولية الأخرى ذات الصلة التي تعمل في مجال التشريعات الوطنية لمكافحة الجرائم السيبرانية؛ ودعم جهود الدول الأعضاء في الاتحاد على الصعيدين الوطني والإقليمي لبناء القدرات اللازمة للحماية من التهديدات والجرائم السيبرانية وذلك بالتعاون فيما بينها بما يتفق مع التشريعات الوطنية للدول الأعضاء المشار إليها أعلاه، ومساعدة الدول الأعضاء، لا سيما البلدان النامية، في وضع تدابير قانونية مناسبة وقابلة للتطبيق تتصل بالحماية من التهديدات السيبرانية على المستويات الوطنية والإقليمية والدولية، وإرساء التدابير التقنية والإجرائية التي تهدف إلى تأمين البنى التحتية الوطنية لتكنولوجيا المعلومات والاتصالات مع الأخذ بعين الاعتبار عمل لجان الدراسات ذات الصلة في قطاع تقييس الاتصالات، وعمل المنظمات الأخرى ذات الصلة حسب الاقتضاء؛ وإنشاء الهياكل التنظيمية مثل أفرقة الاستجابة للحوادث الحاسوبية، لتحديد التهديدات السيبرانية وإدارتها والتعامل معها، ووضع آليات التعاون على المستويين الإقليمي والدولي؛

3 بتقديم الدعم المالي والإداري اللازم لهذه المشاريع في حدود الموارد الحالية، والتماس موارد إضافية (نقدية وعينية) لتنفيذ هذه المشاريع من خلال اتفاقات الشراكة؛

4 بتأمين تنسيق عمل هذه المشاريع في سياق مجمل الأنشطة التي يقوم بها الاتحاد بناء على دوره كجهة تنسيق/تسهيل في خط العمل جيم5 للقمة العالمية لمجتمع المعلومات، والتخلص من أي ازدواجية في العمل فيما يتعلق بهذا الموضوع الهام مع أنشطة الأمانة العامة وقطاع تقييس الاتصالات؛

5 بتنسيق عمل هذه المشاريع مع أعمال لجان دراسات قطاع تنمية الاتصالات بشأن هذا الموضوع، ومع أنشطة البرامج ذات الصلة ومع الأمانة العامة؛

6 بمواصلة التعاون مع المنظمات ذات الصلة بغية تبادل أفضل الممارسات ونشر المعلومات من خلال ورش عمل ودورات تدريبية مشتركة على سبيل المثال؛

7 بتحديد أفضل الممارسات لتطوير المؤهلات والمسارات المهنية في مجال الأمن السيبراني وزيادة وعي أعضاء الاتحاد بها؛

8 بدعم أعمال لجنة الدراسات 17 ولجان الدراسات الأخرى لقطاع تقييس الاتصالات من خلال تعزيز وتسهيل الدول الأعضاء في الاتحاد وأعضاء القطاعات، خاصةً من البلدان النامية، تنفيذ التوصيات الموافق عليها لقطاع تقييس الاتصالات المتعلقة بالأمن؛

9 بدعم الدول الأعضاء في الاتحاد في وضع استراتيجياتها الوطنية و/أو الإقليمية للأمن السيبراني، من أجل بناء القدرات الوطنية للتصدي للتهديدات السيبرانية والحماية منها ضمن مبادئ التعاون الدولي بما يتفق والهدف 2 لخطة عمل بوينس آيرس للمؤتمر العالمي لتنمية الاتصالات؛

10 بدعم الأعضاء في تنمية المهارات البشرية وبناء القدرات لتعزيز الأمن السيبراني؛

11 بدعم الأعضاء لمعالجة النقص في مهارات الأمن السيبراني من خلال تشجيع الناس على الانخراط في المهن المتعلقة بالأمن السيبراني وتيسير توظيف النساء والرجال في مجال الأمن السيبراني؛

12 بالاحتفاظ بمستودع لأفضل الممارسات بشأن التدابير التي تيسر وتشجع الناس، لا سيما النساء والفتيات، على اختيار مسار وظيفي في مجال الأمن السيبراني، وتطوير هذا المستودع وتعزيزه؛

13 بدعم الأعضاء في أنشطة تقييم المخاطر المتعلقة بالأمن السيبراني؛

14 بدعم الدول الأعضاء في تحديد أفضل الممارسات بشأن الإبلاغ بشكل مسؤول عن مواطن الضعف في تكنولوجيا المعلومات والاتصالات؛

15 بتقديم تقرير سنوي إلى المجلس عن هذه الأنشطة وعرض مقترحات حسب الاقتضاء،

يكلف كذلك مدير مكتب تقييس الاتصالات ومدير مكتب تنمية الاتصالات بأن يقوم كل منهما في نطاق مسؤولياته بما يلي

1 تنفيذ القرارات ذات الصلة الصادرة عن الجمعية العالمية لتقييس الاتصالات لعام 2016 والمؤتمر العالمي لتنمية الاتصالات لعام 2017، بما في ذلك الناتج 2.2 من الهدف 2 من خطة عمل بوينس آيرس، مع تركيز خاص على احتياجات البلدان النامية عند قيامها بجهود من أجل تحسين الأمن السيبراني وبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

2 تحديد وتعزيز توافر المعلومات بشأن بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات بما في ذلك البنية التحتية لتكنولوجيا المعلومات والاتصالات من أجل الدول الأعضاء وأعضاء القطاعات والمنظمات ذات الصلة؛

3 مواصلة تحديد أفضل الممارسات المتعلقة بالمسألة 3/2 بما في ذلك تأسيس أفرقة الاستجابة للحوادث الحاسوبية واستعراض الدليل المرجعي للدول الأعضاء دون تكرار العمل الجاري في المسألة 3/2 لقطاع تنمية الاتصالات، من أجل المساهمة في هذه المسألة؛

4 التعاون مع المنظمات ذات الصلة وسائر الخبراء الدوليين والوطنيين، حسب الاقتضاء، من أجل تحديد أفضل الممارسات في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، بما في ذلك إنشاء أفرقة الاستجابة للحوادث الحاسوبية؛

5 اتخاذ الإجراءات الكفيلة بدراسة مسائل جديدة في لجان الدراسات ضمن القطاعات المعنية بإرساء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

6 تحديد وتوثيق الخطوات العملية اللازمة لدعم البلدان النامية في بناء القدرات والمهارات في مجال الأمن السيبراني، مع مراعاة التحديات المحددة التي تواجهها؛

7 مراعاة التحديات التي يواجهها جميع أصحاب المصلحة، خاصةً في البلدان النامية، من أجل بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات وتحديد الخطوات التي يمكن أن تساعد في التصدي لها؛

8 دعم الدول الأعضاء في تحديد الخطوات الأساسية التي ينبغي للجميع اتخاذها لحماية أنفسهم من المخاطر السيبرانية، مثل استخدام كلمات السر القوية، والاستيقان بعامليْن وتحديث البرمجيات بشكل منتظم، وتشجيع ودعم أعضاء الاتحاد وغيرهم من أصحاب المصلحة للترويج لهذه الخطوات لدى الجمهور؛

9 تحديد وتوثيق الخطوات العملية اللازمة لتعزيز الأمن في استخدام تكنولوجيا المعلومات والاتصالات على الصعيد الدولي، بما في ذلك مفهوم أن ينظر إلى الأمن كعملية مستمرة ومتكررة، استناداً إلى نُهج "الأمن في التصميم" وغيرها من الممارسات والمبادئ التوجيهية والتوصيات المقبولة على نطاق واسع، التي يمكن أن تقرر الدول الأعضاء وأصحاب المصلحة الآخرون تطبيقها لتحسين قدرتها على مكافحة التهديدات السيبرانية والهجمات السيبرانية، بما في ذلك نهج دينامي وتكراري قائم على المخاطر ينعكس فيه الطابع المتطور للتهديدات ومواطن الضعف، وتعزيز التعاون الدولي في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، ومع مراعاة البرنامج العالمي للأمن السيبراني (GCA) وفي حدود الموارد المالية المتاحة؛

10 دعم الاستراتيجية والتنظيم والتوعية والتعاون والتقييم وتنمية المهارات؛

11 تقديم الدعم التقني والمالي اللازم في حدود الموارد المتاحة في الميزانية وفقاً للقرار 58 (المراجَع في دبي، 2012) للجمعية العالمية لتقييس الاتصالات؛

12 تشجيع مشاركة الخبراء في أنشطة الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

13 تعبئة الموارد المناسبة من خارج الميزانية العادية للاتحاد من أجل تنفيذ هذا القرار، لمساعدة البلدان النامية؛

14 دعم البلدان النامية ومساعدتها في تشجيع وتسهيل تنفيذ توصيات قطاع تقييس الاتصالات المتعلقة بالأمن،

يكلف الأمين العام

وفقاً لمبادرته في هذا الشأن:

1 بتقديم تقرير إلى المجلس، مع مراعاة أنشطة القطاعات الثلاثة عن تنفيذ وفعالية خطة العمل لتعزيز دور الاتحاد في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

2 بالتعاون مع المنظمات الدولية ذات الصلة بما في ذلك من خلال اعتماد مذكرات التفاهم التي تخضع لموافقة المجلس في هذا الصدد، وفقاً للقرار 100 (مينيابوليس، 1998) لمؤتمر المندوبين المفوضين،

يطلب من مجلس الاتحاد

أن يدرج تقرير الأمين العام في الوثائق المرسلة إلى الدول الأعضاء وفقاً للرقم 81 من الاتفاقية.

يدعو الدول الأعضاء

1 إلى النظر في الانضمام إلى المبادرات الدولية والإقليمية المختصة المناسبة التي تعزز الأطر التشريعية الوطنية ذات الصلة بأمن شبكات المعلومات والاتصالات؛

2 إلى التعاون بشكل وثيق على تعزيز التعاون الإقليمي والدولي، مع الأخذ في الاعتبار القرار 45 (المراجَع في دبي، 2014) بهدف تعزيز الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، من أجل تخفيف المخاطر والتهديدات؛

3 إلى دعم مبادرات الاتحاد بشأن الأمن السيبراني، بما في ذلك الرقم القياسي العالمي للأمن السيبراني (GCI) والمنصة العالمية بشأن قدرة الشبكات على الصمود، من أجل تشجيع الاستراتيجيات الحكومية وتبادل المعلومات عن الجهود المبذولة عبر الصناعات والقطاعات؛

4 إلى إبلاغ الأمين العام عن الأنشطة ذات الصلة المتعلقة بهذا القرار فيما يتعلق بالثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

5 إلى الاستفادة من موارد المبادرات الوطنية والإقليمية والدولية المتعلقة بالأمن السيبراني حول العالم ومن الدعم الذي تقدمه وأفضل ممارساتها، وذلك عن طريق الصفحة الإلكترونية للأمن السيبراني للاتحاد؛

6 إلى التعاون مع المنظمات ذات الصلة، عن طريق تبادل أفضل الممارسات في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات بما في ذلك إنشاء وتنفيذ أفرقة وطنية للاستجابة للحوادث الحاسوبية؛

7 إلى مواصلة إذكاء الوعي من خلال نشر أفضل الممارسات والسياسات التي تم تنفيذها من أجل زيادة القدرة على وضع سياسات ملائمة لحماية المستخدمين وتعزيز الثقة في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات؛

8 تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات بطريقة تتيح تنمية المجتمع المدني وتدعم تحقيق مستويات أعلى من المنافع الاجتماعية والاندماج الاجتماعي،

يدعو الدول الأعضاء وأعضاء القطاعات والمنتسبين إليها

1 إلى تقديم مساهمات بشأن هذا الموضوع إلى لجان الدراسات ذات الصلة في الاتحاد والمساهمة في أي أنشطة أخرى يتولى الاتحاد مسؤوليتها؛

2 إلى المساهمة في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات على الأصعدة الوطنية والإقليمية والدولية وذلك بالاضطلاع بأنشطة على النحو الموضح في الوثائق الختامية للقمة في القمة العالمية لمجتمع المعلومات، وبيان الحدث الرفيع المستوى (WSIS+10) بشأن تنفيذ نتائج القمة العالمية لمجتمع المعلومات ورؤية الحدث (WSIS+10) للقمة العالمية بعد 2015، والوثيقة الختامية للاجتماع الرفيع المستوى للجمعية العامة بشأن الاستعراض العام لتنفيذ نتائج القمة العالمية لمجتمع المعلومات، والمساهمة في إعداد تلك الأنشطة وتنفيذها؛

3 إلى زيادة الوعي بين أصحاب المصلحة كافة، بما في ذلك المنظمات وفرادى المستعملين بأهمية تعزيز الأمن السيبراني، بما في ذلك تنفيذ تدابير الحماية الأساسية؛

4 إلى تشجيع تطوير البرامج التعليمية والتدريبية لتعزيز وعي المستخدم بشأن المخاطر في الفضاء السيبراني والخطوات التي يمكن أن يتخذها المستخدمون من أجل حماية أنفسهم؛

5 إلى إدراج نهج دينامي وتكراري قائم على المخاطر للتصدي للتهديدات ومواطن الضعف الآخذة في التطور، وتعزيز ثقافة ينظر فيها إلى الأمن على أنه عملية مستمرة ومتكررة يجب أن يشملها تطوير ونشر التكنولوجيات وتطبيقاتها منذ البداية ويجب الاستمرار فيها على مدى دورة حياتها، في إطار جهودها الرامية إلى بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

6 إلى تعزيز المبادرات الرامية إلى تشجيع المزيد من الناس على ممارسة مهنة الأمن السيبراني وتزويدهم بفرص التدريب؛

7 إلى تقديم الدعم بحيث تتمكن النساء والفتيات من القيام بدراسات والعمل في مجال الأمن السيبراني؛

8 إلى المساهمة في مستودع الاتحاد لأفضل الممارسات بشأن التدابير التي تيسر وتشجع المزيد من الناس، ولا سيما النساء والفتيات، على اختيار مسار وظيفي في مجال الأمن السيبراني؛

9 إلى التعاون حسب الاقتضاء للتغلب على المشاكل التي تضعف الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات ومنعها؛

10 إلى تحديد الخطوات الأساسية التي ينبغي للجميع اتخاذها لحماية أنفسهم من المخاطر السيبرانية والقيام بدور فعال في تعزيزها.

ـــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ